

AFFIDAVIT OF BRYAN MOLNAR

STATE OF WASHINGTON)
) ss
 COUNTY OF PIERCE)

I, Bryan Molnar, a Special Agent with the United States Secret Service, Seattle, Washington, having been duly sworn, state as follows:

INTRODUCTION AND AFFIANT BACKGROUND

1. I am a Special Agent (SA) with the United States Secret Service (Secret Service) and have been so since March 1, 2010. I am currently assigned to the Seattle Field Office. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography and material involving the sexual exploitation of minors, in violation of 18 U.S.C. §§ 2251, 2252(a), and 2252A(a). I am a graduate of the Federal Law Enforcement Training Center located in Glynco, Georgia, and the Secret Service Special Agent Training Program located in Beltsville, Maryland. Additionally, I am a graduate of the Cleveland Heights Police Academy, located in Cleveland Heights, Ohio. Prior to my employment with the Secret Service, I was a commissioned Law Enforcement Officer for more than six years, serving as a patrol officer in Ohio and as a sworn criminal investigator in Arizona. I have a Bachelor of Arts degree from Case Western Reserve University and a Master of Science degree from Boston University. In the course of my law enforcement career, I have investigated crimes ranging from narcotics, sexual assaults, and homicide, to counterfeit currency and multiple types of fraud. As part of my training with the Secret Service, I have received instruction on the investigation of financial crimes, including credit/debit card fraud, mail and wire fraud, access device fraud, and identity theft. I have also completed specialized training in the investigation of electronic crimes involving the use of computers and other electronic devices. I have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256(8)). I have

AFFIDAVIT OF BRYAN MOLNAR - 1

UNITED STATES ATTORNEY
 1201 PACIFIC AVENUE, SUITE 700
 TACOMA, WASHINGTON 98402
 (253) 428-380

1 participated in the execution of search warrants involving child exploitation and/or child
2 pornography offenses, and in the search and seizure of computers and other digital
3 devices. I am a member of the Seattle Internet Crimes Against Children (ICAC) Task
4 Force, and work with other federal, state, and local law enforcement personnel in the
5 investigation and prosecution of crimes involving the sexual exploitation of children. I
6 am also assigned to the Joint Terrorism Task Force.

7 2. I make this Affidavit in support of applications under Rule 41 of the
8 Federal Rules of Criminal Procedure for (1) a warrant to search the premises known as
9 2015 68th Ave NE, Tacoma, Washington 98422 (the "SUBJECT PREMISES"), more
10 fully described in Attachment A1 to this Affidavit, fully incorporated herein by reference,
11 for the items described in Attachment B1 to this Affidavit, fully incorporated herein by
12 reference; (2) a warrant to search the email account "kaiden.evinlyle@gmail.com,"
13 controlled by Google, Inc. (Google), as well as all other subscriber and log records
14 associated with this email account, including any associated Google Drive cloud storage
15 accounts (collectively, the "SUBJECT EMAIL ACCOUNT"), more fully described in
16 Attachment A2 to this Affidavit, for the items listed in Attachment B2 to this Affidavit,
17 fully incorporated herein by reference; and (3) a warrant to search two cellphones
18 currently being held at the Pierce County Jail, more fully described in Attachment A3 to
19 this Affidavit, fully incorporated herein by reference ("EVINLYLE's PHONES"), for the
20 items described in Attachment B3 to this Affidavit, fully incorporated herein by
21 reference; all for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251
22 (Production of Child Pornography/Sexual Exploitation of Children), 2252(a)(2) (Receipt
23 or Distribution of Child Pornography) and 2252(a)(4)(B) (Possession of Child
24 Pornography).

25 3. The facts set forth in this Affidavit are based on my own personal
26 knowledge; knowledge obtained from other individuals during my participation in this
27 investigation, including other law enforcement officers; interviews of cooperating
28 witnesses; review of documents and records related to this investigation; communications

AFFIDAVIT OF BRYAN MOLNAR - 2

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-380

1 with others who have personal knowledge of the events and circumstances described
2 herein; and information gained through my training and experience.

3 4. Because this Affidavit is submitted for the limited purpose of establishing
4 probable cause in support of the applications for the search warrants, it does not set forth
5 each and every fact that I or others have learned during the course of this investigation. I
6 have set forth only the facts that I believe are relevant to the determination of probable
7 cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§
8 2251 (Production of Child Pornography/Sexual Exploitation of Children), 2252(a)(2)
9 (Receipt or Distribution of Child Pornography) and 2252(a)(4)(B) (Possession of Child
10 Pornography), will be found at the SUBJECT PREMISES, in the SUBJECT EMAIL
11 ACCOUNT, and on EVINLYLE's PHONES.

12 **SUMMARY OF INVESTIGATION**

13 5. On May 8, 2012, Tacoma Police Department (TPD) Detective Scott Yenne
14 was assigned a case involving allegations of child molestation against a nine-year-old
15 female child with the initials T.S. T.S.'s full name is known to me, but is not included
16 for purposes of this Affidavit. The alleged perpetrator, KAIDEN EVINLYLE, was
17 friends with T.S.'s mother, a woman with the initials R.S. R.S.'s full name is known to
18 me, but is not included for purposes of this Affidavit. R.S. met KAIDEN EVINLYLE on
19 a website for single parents. They became friends and began to have playdates with their
20 children, including overnight sleepovers at EVINLYLE's residence (the SUBJECT
21 PREMISES). The friendship began in November 2010, and continued until
22 approximately April 2012. T.S. told her mother that, when she was seven to eight years
23 old, EVINLYLE did inappropriate things with her at the SUBJECT PREMISES,
24 including "French kissing" her. According to T.S., EVINLYLE explained the kiss to her,
25 then kissed her and put his tongue into her mouth. T.S. described the kiss as a secret she
26 had with EVINLYLE. During a later post-Miranda interview, EVINLYLE admitted to
27 kissing T.S. on the lips several times. EVINLYLE also admitted to showing T.S. a
28 French kiss one time, but stated that it was a demonstration and not sexual in nature.

1 6. T.S. described another occasion when she was spending the night at the
2 SUBJECT PREMISES and took a bath in the bathroom. EVINLYLE came into the
3 bathroom and asked to wash her hair. T.S. said EVINLYLE took his clothes off and got
4 into the bathtub with her naked. T.S. said he rubbed her chest area and touched her upper
5 thighs with his hands, very close to her "private area." During a later post-Miranda
6 interview, EVINLYLE stated he never touched T.S.'s genital area and never penetrated
7 her. EVINLYLE stated "if anything it's a testament to my self-control," and went on to
8 say most guys would have had sexual contact in that situation.

9 7. T.S. said most of the time she went to the SUBJECT PREMISES to spend
10 the night she and EVINLYLE's daughter, E.M., would fall asleep in the living room.
11 E.M.'s full name is known to me, but is not included for purposes of this Affidavit. T.S.
12 said in the morning she would wake up in EVINLYLE's bedroom on his bed. T.S. said
13 one of those nights she woke up in that bed and EVINLYLE was on top of her naked,
14 sweating and making noises. T.S. said he was doing "push-ups" on her, forcing his
15 "private area" to hers and making contact. T.S. said EVINLYLE held a plastic bag over
16 his private area preventing skin to skin body contact. T.S. said she was clothed at the
17 time, but EVINLYLE's private area pushed against her underwear. T.S. said she
18 pretended to be asleep and didn't say anything because she was scared. During a later
19 post-Miranda interview, EVINLYLE stated one night T.S. came into his room, laid down
20 next to him, and started to tickle and play with him. EVINLYLE said it was possible he
21 got an erection and he pushed her away. EVINLYLE also said it was possible his
22 genitals and hers touched, but he was wearing boxers and she was wearing underwear.
23 When asked if he was attracted to T.S., EVINLYLE stated it was natural for a man to be
24 attracted to a woman. When asked if T.S. was a woman, EVINLYLE replied, "Well
25 she's a female." EVINLYLE also stated men can be attracted to girls.

26 8. T.S. also said EVINLYLE would take photographs of her and E.M. in
27 "fairy" outfits. T.S. said EVINLYLE made the outfits and would pose the girls on his
28 bed. T.S. described EVINLYLE's bedroom as having pictures of partially nude fairies on

1 the wall, and described the bed as a four-posted canopied-style bed. T.S. said
2 EVINLYLE had a changing room where she and E.M. would get into costume and there
3 were computer monitors in that room.

4 9. During an interview with R.S., T.S.'s mother, R.S. confirmed
5 EVINLYLE's address at the SUBJECT PREMISES and described his residence. She
6 said EVINLYLE seemed more interested in T.S. coming over to his house than in her
7 coming over. R.S. went on to say she saw a computer monitor in EVINLYLE's living
8 room on which a picture of T.S. was the screensaver and on the desktop of which was a
9 file folder with T.S.'s name on it. When she confronted him about it, EVINLYLE
10 admitted he took photographs of T.S. EVINLYLE showed R.S. pictures of T.S. dressed
11 as a fairy on his bed. R.S. stated she felt uncomfortable about it because some of the
12 pictures appeared sexual in nature.

13 10. The investigation described in Paragraphs 5-9 above was not TPD's first
14 contact with EVINLYLE. In 2007, TPD investigated EVINLYLE after a coworker
15 reported finding inappropriate pictures on EVINLYLE's computer. EVINLYLE had
16 asked his coworker to help him repair the computer, and in the process the coworker
17 found pictures of what he believed to be EVINLYLE's then five- or six-year-old
18 daughter, E.M., with her legs spread, exposing her underwear. EVINLYLE admitted to
19 TPD that he took the pictures, and stated he was "an artist." The investigation was closed
20 without any charges being filed.

21 11. Based on Detective Yanne's investigation in May 2012, described above in
22 Paragraphs 5-9, TPD obtained a search warrant for the SUBJECT PREMISES and
23 executed it on June 28, 2012. At that time, EVINLYLE was the only occupant of the
24 SUBJECT PREMISES. Law enforcement seized three computers, photographs, external
25 hard drives, DVDs, cameras, little girl's underwear, and documents of dominion and
26 control from the SUBJECT PREMISES. As described further below, the three computers
27 are still in law enforcement custody and have not been returned to EVINLYLE.
28

1 EVINLYLE also participated in a voluntary, Mirandized interview with detectives
2 wherein he made the statements described above in Paragraphs 5-7.

3 12. EVINLYLE was charged initially in Pierce County on December 28, 2012,
4 with two counts of First Degree Child Molestation and one count of Communication
5 With a Minor for Immoral Purposes; those charges were subsequently amended to
6 aggravate the child molestation counts and an additional charge, Second Degree
7 Possession of Depictions of Minors Engaged in Sexually Explicit Conduct, was added.
8 After a series of court hearings, trial was scheduled to begin on November 4, 2013.
9 EVINLYLE failed to appear for trial, and a bench warrant issued. He was arrested on
10 November 6, 2013, and taken into custody. When he was booked into the Pierce County
11 Jail on November 6, 2013, two phones were taken from him (EVINLYLE's PHONES)
12 and placed into property, a black Samsung Galaxy Note 2 and a red and white Samsung.
13 EVINLYLE's PHONES are still at the Pierce County Jail. Both of EVINLYLE's
14 PHONES bear markings on them indicating that they were purchased from T-Mobile.
15 At the time of his arrest, EVINLYLE provided a telephone number of 206-355-7426.
16 EVINLYLE has been in custody since November 6, 2013. Based on my observations of
17 the SUBJECT PREMISES on three occasions since then, the SUBJECT PREMISES are
18 unoccupied.

19 13. On November 12, 2013, I received information that an individual named
20 KAIDEN EVINLYLE, using a PayPal account, had made suspected child pornography-
21 related purchases from the website "nudistwonderland.com." Another federal law
22 enforcement agency is currently investigating the "nudistwonderland.com" website in
23 relation to child pornography crimes.

24 14. On November 12, 2013, using an undercover computer, I was able to go
25 onto the website "nudistwonderland.com." I observed the homepage of the website to
26 have over 15 images of more than 20 nude children. While the website states it is selling
27 nudist pictures, I did not observe a single picture of an adult on the homepage. Instead,
28 the images I observed were of prepubescent children, many posed outdoors in various

1 poses. Some of the children were posed provocatively; I observed one image of what
2 appears to be a prepubescent female facing a wall with her buttocks out, looking back at
3 the camera over her shoulder. Some of the images I observed depict young males with
4 erect and partially-erect penises. Many of the females depicted in the images I observed
5 on the homepage did not have pubic hair, breast or hip development, or musculature
6 found in a legal-aged adult. Based on my training, experience and conversations with
7 other investigators who work cases pertaining to child pornography, it is common for
8 people who purchase, trade, and distribute child pornography to try to justify it as legal
9 by claiming they are "nudist" or "naturalist" images. However, based on my training and
10 experience, if this were a legitimate nudist website, it would be common to see images of
11 adults as well. Moreover, in order to obtain access to the folders of images on this
12 website, an individual is required to send a check or money order, along with a valid
13 email address. Upon receipt of the funds, the website administrator states that the
14 individual will then receive an email with a link from which the folders on the homepage
15 can be accessed and their contents downloaded.

16 15. Information received from PayPal pursuant to a subpoena showed that
17 KAIDEN EVINLYLE made a \$50.00 purchase from the website
18 "nudistwonderland.com" for "All Folders" on July 18, 2013. PayPal records indicated
19 EVINLYLE made this purchase using the SUBJECT EMAIL ACCOUNT from IP
20 address 184.78.176.135. I queried publicly available websites and found this IP address
21 is hosted by Clear Wireless, and was being used south of Seattle. PayPal records also
22 confirmed EVINLYLE's credit card number and address at the SUBJECT PREMISES,
23 and an associated telephone number for EVINLYLE's PayPal account of 206-355-7426,
24 the same number he provided to law enforcement as being his.

25 16. In November of 2013, I also performed an open source search on the name
26 "KAIDEN EVINLYLE" and located the following post made on October 28, 2013, to the
27 website "[http://sentencing.typepad.com/sentencing_law_and_policy/2012/03/from-peer-](http://sentencing.typepad.com/sentencing_law_and_policy/2012/03/from-peer-to-peer-networks-to-cloud-computing-how-technology-is-redefining-child-pornography-)
28 [to-peer-networks-to-cloud-computing-how-technology-is-redefining-child-pornography-](http://sentencing.typepad.com/sentencing_law_and_policy/2012/03/from-peer-to-peer-networks-to-cloud-computing-how-technology-is-redefining-child-pornography-)

1 laws.html.” Based on the uniqueness of KAIDEN EVINLYLE’s name, and the content
2 of the post, I believe it was written by the same KAIDEN EVINLYLE who lives at the
3 SUBJECT PREMISES, uses the SUBJECT EMAIL ACCOUNT, and owns
4 EVINLYLE’s PHONES. On October 28, 2013, EVINLYLE posted the following
5 comment to the website. Any typographical or grammatical errors are in the original
6 post.

7 I’m very concerned about the lack of proper definition of child
8 pornography. Police seized my computers and stated that there were
9 no images of child pornography on my computers but that they
10 would do a deep search of my hard drive. The first deep search they
11 said they have 500 images that may be child pornography. A month
12 later they said they have 250 images that are child pornography.
13 Another month later they said well actually we have 15 images that
14 are child pornography. And so out of 70,000 pictures they dug up
15 the 15 worst they could find to present to the jury and try convict
16 me. The thing is I am completely and vehemently against child
17 pornography! But I have a great appreciation for beauty. All the
18 sites that I got pictures from were simply modeling sites with no
19 sexual contact whatsoever. Laws were clearly posted on sites and
20 clearly marked NOT CHILD PORNOGRAPHY. Not to mention
21 these sites are all still up and running and claim to be legitimate and
22 legal. I did not ever consider any of the pictures downloaded to be
23 child pornography. It appears that Washington State defines child
24 pornography differently than the national law does. I did not know
25 that. I never had any intention of breaking any laws. I believe very
26 strongly in the freedom of self-expression. All the models had full
27 parental permission and they all seemed to really enjoy what they
28 did. I think that child pornography should be more clearly defined
as sexual contact. Otherwise the authorities will inevitably trample
on people’s rights to freedom of expression.

17. After conducting this open source search, I ran the name “KAIDEN
EVINLYLE” through a law enforcement database and found information about the TPD
investigations described in Paragraphs 5-11 above. On November 13, 2013 I contacted
Detective Yenne, who explained the focus of the current investigation, i.e., the
allegations of child molestation against EVINLYLE. Detective Yenne further told me he

1 had seized EVINLYLE's computers on June 28, 2012, and that the computers had not
2 been returned to EVINLYLE. This means that EVINLYLE's purchases from the website
3 "nudistwonderland.com," and his posting to the website named in Paragraph 15, above,
4 were not only made after his contact with law enforcement on June 28, 2012, but had to
5 have been made from an Internet-accessible device, e.g., EVINLYLE's PHONES,
6 obtained after law enforcement seized the computers at the SUBJECT PREMISES on
7 June 28, 2012.

8 18. On December 6, 2013, I met with TPD Detective Heath Holden, who
9 performed the forensic examination on the computers and other items seized from the
10 SUBJECT PREMISES. Detective Holden reviewed the results of his forensic
11 examination with me, and stated he located numerous images of what he believed to be
12 child pornography on EVINLYLE's digital devices. Detective Holden stated he found
13 over 50,000 images on all of the media combined, and the majority of the images
14 contained pictures of preteen girls in varying states of dress and many pictures of nude
15 young girls. Detective Holden described the pictures as provocative in nature and the
16 positions of the children as sexually suggestive. Many of these pictures had been
17 downloaded from websites such as "purenudism.com," but some appear to have been
18 produced by EVINLYLE.

19 19. For example, Detective Holden showed me an image of a topless
20 prepubescent girl, who appears to be between eight and ten years old, wearing only bikini
21 bottoms, sitting on the bow of a boat with her legs spread. Based on my training and
22 experience, this image appears to have been downloaded from a website. Detective
23 Holden then showed me a photograph EVINLYLE took of one of his daughter's friends,
24 a young girl with the initials E.L., wearing a life jacket and bikini bottoms posed in the
25 exact same way as the above photograph, sitting in a canoe. E.L.'s full name is known to
26 me, but is not included for purposes of this Affidavit. In the picture EVINLYLE took of
27 E.L., her bikini bottoms are askew and pulled to the side. The next photograph, which
28

1 also appears to have been taken by EVINLYLE, is of E.L., lying on her stomach on the
2 canoe, provocatively looking back at the camera over her shoulder.

3 20. Detective Holden had located other photographs of E.L. on the computer,
4 including a series of photographs of E.L. lying on a hammock with EVINLYLE's
5 daughter, E.M. In these photographs, E.L. is wearing a bikini. There were two
6 photographs of just E.L.'s bikini bottoms, focusing on her vaginal area. Detective
7 Holden had also located other photographs of E.L., based on the same bathing suit, which
8 were taken underwater in a swimming pool and were focused on her genital area.
9 Detective Holden found a third series of photographs of E.L. where she is lying on a bed,
10 wearing a very short dress, and is provocatively posed. The last picture in this series is of
11 E.L. in a hammock with her legs spread. E.L. is not wearing underwear, and her vagina
12 is clearly visible.

13 21. On another computer seized during the search warrant at the SUBJECT
14 PREMISES, Detective Holden located additional pictures of E.L.; these photographs
15 include E.L. posing in underwear and pulling up her shirt as if she is undressing. Also
16 found on this computer was a photograph of a group of naked people, which included an
17 adult male and an approximately five-year-old girl. The adult male is sitting on the floor,
18 touching the five-year-old's vagina. Multiple additional photographs of scantily-clad
19 young girls dressed in their underwear or dressed as fairies, with their legs spread, were
20 located on this computer. Additionally, motivational-type posters were located on this
21 computer, one of which is described as a picture of a young girl, approximately eight
22 years old, with the caption "Pedophiles- Can you really blame them?"

23 22. On January 17, 2014, a subpoena was issued to Google requesting
24 subscriber information for the SUBJECT EMAIL ACCOUNT. Google responded on
25 January 22, 2014, with the following subscriber information:

26	Name:	KAIDEN EVINLYLE
27	Email:	kaidenevinlyle@gmail.com
28	Created on:	February 28, 2007
	Other user names:	[the SUBJECT EMAIL ACCOUNT]

1 On January 22, 2014, I contacted Google to clarify the difference between the first
 2 email address they provided, "kaidenevinlyle@gmail.com," and the SUBJECT EMAIL
 3 ACCOUNT, "kaiden.evinlyle@gmail.com." Google responded on January 23, 2014, and
 4 stated that the Gmail service does not recognize dots as characters within user names, and
 5 that users can add or remove the dots from a Gmail address without changing the actual
 6 destination address. Google provided the following example: the email address
 7 "yourusername@gmail.com" is the same as "your.username@gmail.com" or
 8 "your.user.name@gmail.com."

9 23. The subscriber information provided by Google on January 22, 2014, also
 10 indicated that one of the services used by EVINLYLE in connection with the SUBJECT
 11 EMAIL ACCOUNT is Picasa Web Albums; Picasa is a photo-sharing website. Google
 12 provided an associated telephone number of 206-355-7426, which is the same telephone
 13 number linked to EVINLYLE's PayPal account, and the same telephone number
 14 EVINLYLE provided as his to the Pierce County Jail. Google also provided an IP
 15 history for the SUBJECT EMAIL ACCOUNT. The most recent IP address used to log
 16 into the SUBJECT EMAIL ACCOUNT, on November 6, 2013, at 00:22:18 UTC, was
 17 172.56.33.150. An open source search revealed that this IP address is assigned to T-
 18 Mobile. As noted above in Paragraph 12, EVINLYLE's PHONES both bear markings
 19 indicating they were purchased from T-Mobile. The IP history also included use of IP
 20 address 184.78.176.135 to log into the SUBJECT EMAIL ACCOUNT on October 21,
 21 2013, at 13:12:27 UTC. This is the same IP address used for EVINLYLE's purchase, via
 22 PayPal, from the "nudistwonderland.com" website on July 18, 2013, described above in
 23 Paragraph 15.

24 **DEFINITIONS AND TECHNICAL TERMS**

25 24. Set forth below are some definitions of technical terms, most of which are
 26 used throughout this Affidavit pertaining to the Internet and computers generally.

27 a. **Computers and digital devices:** As used in this Affidavit, the terms
 28 "computer" and "digital device," along with the terms "electronic storage media,"

1 “digital storage media,” and “data storage device,” refer to those items capable of storing,
2 creating, transmitting, displaying, or encoding electronic or digital data, including
3 computers, hard drives, thumb drives, flash drives, memory cards, media cards, smart
4 cards, PC cards, digital cameras and digital camera memory cards, electronic notebooks
5 and tablets, smart phones and personal digital assistants, printers, scanners, and other
6 similar items.

7 b. Internet Protocol (IP) Address: Typically, computers or devices on
8 the Internet are referenced by a unique Internet Protocol address the same way every
9 telephone has a unique telephone number. An IP address consists of four numeric
10 sequences, separated by a period, and each numeric sequence is a whole number between
11 0 and 254. An example of an IP address is 192.168.10.102. Each time an individual
12 accesses the Internet, the computer from which that individual initiates access is assigned
13 an IP address. A central authority provides each Internet Service Provider (ISP) a limited
14 block of IP addresses for use by that ISP’s customers or subscribers. Most ISP’s employ
15 dynamic IP addressing, that is, they allocate any unused IP address at the time of
16 initiation of an Internet session each time a customer or subscriber accesses the Internet.
17 A dynamic IP address is reserved by an ISP to be shared among a group of computers
18 over a period of time. The ISP logs the date, time, and duration of the Internet session for
19 each IP address and can identify the user of that IP address for such a session from these
20 records. Typically, users who sporadically access the Internet via a dial up modem will be
21 assigned an IP address from a pool of IP addresses for the duration of each dial up
22 session. Once the session ends, the IP address is available for the next dial up customer.
23 On the other hand, some ISPs, including some cable providers, employ static IP
24 addressing, that is, a customer or subscriber’s computer is assigned one IP address that is
25 used to identify each and every Internet session initiated through that computer. In other
26 words, a static IP address is an IP address that does not change over a period of time and
27 is typically assigned to a specific computer.

1 c. Hash Value: "Hashing" refers to the process of using a
2 mathematical function, often called an algorithm, to generate a numerical identifier for
3 data. This numerical identifier is called a "hash value." A hash value can be thought of
4 as a "digital fingerprint" for data. If the data is changed, even very slightly (like through
5 the addition or deletion of a comma or a period in a text file), the hash value for that data
6 would change. Therefore, if a file such as a digital photo is a hash value match to a
7 known file, it means that the digital photo is an exact copy of the known file.

8 d. Internet Information Services ("IIS") logs: IIS logs are an
9 integration of several types of log files, or data, related to Internet usage. Examples of
10 data contained in IIS logs include IP address logs, dates and times of access to the
11 Internet, and queries.

12 **SUBJECT'S USE OF ELECTRONIC COMMUNICATION SERVICE**

13 25. As outlined above, KAIDEN EVINLYLE, using the SUBJECT EMAIL
14 ACCOUNT, purchased suspected child pornography from the website
15 "nudistwonderland.com" on July 18, 2013. EVINLYLE conducted this transaction over
16 the Internet after TPD seized a number of computers (which have not been returned to
17 EVINLYLE) from the SUBJECT PREMISES on June 28, 2012. Therefore, I believe
18 EVINLYLE either bought a new computer, or used one of EVINLYLE's PHONES to
19 conduct this transaction. EVINLYLE's PHONES are capable of accessing the Internet.

20 26. I know that Google, the entity which controls the SUBJECT EMAIL
21 ACCOUNT, offers over 10 GB of free storage space per email address. This allows
22 users to store a large amount of emails and other related content. Google Drive (formerly
23 known as Google Docs) is a free online "cloud" storage that allows users to share files
24 from any device. With Google Drive, a user can share files in lieu of sending email
25 attachments. Picasa Web Albums (also known as Google+ Photos) is a photo-sharing
26 website owned by Google that allows users to post and share images with other
27 individuals. Google also offers other distinct services, including video chat. All of these
28 services are very useful tools that EVINLYLE, using the SUBJECT EMAIL ACCOUNT,

1 could be using to store and share images of child pornography. Google also allows its
2 users, through its mobile services, to access their email account(s), stored images, and
3 other content at any time from any computer with Internet access.

4 **PRIOR EFFORTS TO OBTAIN EVIDENCE**

5 27. Any other means of obtaining the necessary evidence to prove the elements
6 of computer/Internet-related crimes, for example, a consent search, could result in an
7 unacceptable risk of the loss/destruction of the evidence sought. If agents pursued a
8 consent-based interview of and/or a consent-based search of KAIDEN EVINLYLE's
9 digital media at the SUBJECT PREMISES and/or EVINLYLE's PHONES, EVINLYLE
10 could rightfully refuse to give consent and subsequently destroy all evidence of the crime
11 before agents could return with a search warrant, a situation which other law enforcement
12 agents I have spoken with have personally experienced in previous child exploitation
13 investigations. Based on my knowledge, training and experience, the only effective
14 means of collecting and preserving the required evidence in this case is through a search
15 warrant.

16 28. I understand that the contents of the SUBJECT EMAIL ACCOUNT can
17 only be obtained in the Ninth Circuit by means of a search warrant issued under authority
18 of 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), and Federal Rule of Criminal
19 Procedure 41(e)(2)(b). To my knowledge, there have been no prior attempts to secure a
20 search warrant to search and seize these records.

21 29. Based on my experience and training, it is not uncommon for technically
22 sophisticated criminals to use encryption or programs to destroy data that can be
23 triggered remotely or by a pre-programed event to keystroke, or other sophisticated
24 techniques to hide data. In this case, the data sought from the SUBJECT EMAIL
25 ACCOUNT is stored on a server belonging to Google. If that data is accessed and
26 deleted by the user, by either deleting the emails or any associated contact lists, the
27 content would not be retrievable. Unlike traditional computer forensics where a hard
28 drive can be searched and deleted documents recovered, information stored in an

1 enterprise storage system is irretrievable once it has been deleted. Further, since this
2 information is accessible from anywhere that KAIDEN EVINLYLE can obtain an
3 Internet connection to log on to the account, he could delete this information in a matter
4 of minutes. Moreover, if agents ask EVINLYLE for consent to search the SUBJECT
5 EMAIL ACCOUNT, he may refuse to consent to such a search and then destroy evidence
6 in the SUBJECT EMAIL ACCOUNT before agents are able to obtain a search warrant.

7 TECHNICAL BACKGROUND

8 30. As part of my training, I have become familiar with the Internet, a global
9 network of computers and other electronic devices that communicate with each other
10 using various means, including standard telephone lines, high speed telecommunications
11 links (e.g., copper and fiber optic cable), and wireless transmissions, including satellite.
12 Due to the structure of the Internet, connections between computers on the Internet
13 routinely cross state and international borders, even when the computers communicating
14 with each other are in the same state. Individuals and entities use the Internet to gain
15 access to a wide variety of information; to send information to, and receive information
16 from, other individuals; to conduct commercial transactions; and to communicate via
17 email.

18 31. I know, based on my training and experience, that many cellular phones
19 (referred to herein generally as "smart phones") have the capability to access the Internet
20 and store information, such as videos and images. As a result, an individual using a
21 smart phone can send, receive, and store files, including child pornography, without
22 accessing a personal computer or laptop. An individual using a smart phone can also
23 easily plug the device into a computer, via a USB cable, and transfer data files from one
24 digital device to another. Many people generally carry their smart phone on their person;
25 recent investigations in this District have resulted in the discovery of child pornography
26 files on smart phones which were carried on an individual's person at the time the phones
27 were seized.

1 32. As set forth above and in Attachment B1 to this Affidavit, I seek
2 permission to search for and seize evidence, fruits, and instrumentalities of the above
3 referenced crimes that might be found at the SUBJECT PREMISES or on EVINLYLE's
4 PHONES, in whatever form they are found. It has been my experience that individuals
5 involved in child pornography often prefer to store images of child pornography in
6 electronic form. The ability to store images of child pornography in electronic form
7 makes digital devices, examples of which are enumerated in Attachment B1 to this
8 Affidavit, an ideal repository for child pornography because the images can be easily sent
9 or received over the Internet. As a result, one form in which these items may be found is
10 as electronic evidence stored on a digital device.

11 a. Based upon my knowledge, training, and experience in child
12 exploitation and child pornography investigations, and the experience and training of
13 other law enforcement officers with whom I have had discussions, I know that computers
14 and computer technology have revolutionized the way in which child pornography is
15 collected, distributed, and produced. Prior to the advent of computers and the Internet,
16 child pornography was produced using cameras and film, resulting in either still
17 photographs or movies. The photographs required darkroom facilities and a significant
18 amount of skill in order to develop and reproduce the images. As a result, there were
19 definable costs involved with the production of pornographic images. To distribute these
20 images on any scale also required significant resources. The photographs themselves
21 were somewhat bulky and required secure storage to prevent their exposure to the public.
22 The distribution of these images was accomplished through a combination of personal
23 contacts, mailings, and telephone calls, and compensation would follow the same paths.
24 More recently, through the use of computers and the Internet, distributors of child
25 pornography use membership based/subscription based websites to conduct business,
26 allowing them to remain relatively anonymous.

27 b. In addition, based upon my own knowledge, training, and experience
28 in child exploitation and child pornography investigations, and the experience and

1 training of other law enforcement officers with whom I have had discussions, I know that
2 the development of computers has also revolutionized the way in which those who seek
3 out child pornography are able to obtain this material. Computers serve four basic
4 functions in connection with child pornography: production, communication, distribution,
5 and storage. More specifically, the development of computers has changed the methods
6 used by those who seek to obtain access to child pornography as described in
7 subparagraphs (c) through (f) below.

8 c. Producers of child pornography can now produce both still and
9 moving images directly from the average video or digital camera. These still and/or
10 moving images are then uploaded from the camera to the computer, either by attaching
11 the camera to the computer through a USB cable or similar device, or by ejecting the
12 camera memory card from the camera and inserting it into a card reader. Once uploaded
13 to the computer, the images can then be stored, manipulated, transferred, or printed
14 directly from the computer. Images can be edited in ways similar to those by which a
15 photograph may be altered. Images can be lightened, darkened, cropped, or otherwise
16 manipulated. Producers of child pornography can also use a scanner to transfer printed
17 photographs into a computer-readable format. As a result of this technology, it is
18 relatively inexpensive and technically easy to produce, store, and distribute child
19 pornography. In addition, there is an added benefit to the pornographer in that this
20 method of production does not leave as large a trail for law enforcement to follow.

21 d. The Internet allows any computer to connect to another computer.
22 By connecting to a host computer, electronic contact can be made to literally millions of
23 computers around the world. A host computer is one that is attached to a network and
24 serves many users. Host computers, including ISPs, allow email service between
25 subscribers and sometimes between their own subscribers and those of other networks.
26 In addition, these service providers act as a gateway for their subscribers to the Internet.
27 Having said that, however, this application does not seek to reach any host computers.
28

1 This application seeks permission only to search the computers and digital devices found
2 at the SUBJECT PREMISES, and to search EVINLYLE's PHONES.

3 e. The Internet allows users, while still maintaining anonymity, to
4 easily locate (i) other individuals with similar interests in child pornography, and (ii)
5 websites that offer images of child pornography. Those who seek to obtain images or
6 videos of child pornography can use standard Internet connections, such as those
7 provided by businesses, universities, and government agencies, to communicate with
8 each other and to distribute child pornography. These communication links allow
9 contacts around the world as easily as calling next door. Additionally, these
10 communications can be quick, relatively secure, and as anonymous as desired. All of
11 these advantages, which promote anonymity for both the distributor and recipient, are
12 well known and are the foundation of transactions involving those who wish to gain
13 access to child pornography over the Internet. Sometimes the only way to identify both
14 parties and verify the transportation of child pornography over the Internet is to examine
15 the distributor's/recipient's computer, including the Internet history and cache to look for
16 "footprints" of the websites and images accessed by the distributor/recipient.

17 f. The computer's capability to store images in digital form makes it an
18 ideal repository for child pornography. The size of the electronic storage media
19 (commonly referred to as a "hard drive") used in home computers has grown
20 tremendously within the last several years. Hard drives with the capacity of 500
21 gigabytes are not uncommon. These drives can store thousands of images at very high
22 resolution. Magnetic storage located in host computers adds another dimension to the
23 equation. It is possible to use a video camera to capture an image, process that image in a
24 computer with a video capture board, and save that image to storage elsewhere. Once
25 this is done, there is no readily apparent evidence at the "scene of the crime." Only with
26 careful laboratory examination of electronic storage devices is it possible to recreate the
27 evidence trail.
28

1 33. Based upon my knowledge, experience, and training in child pornography
2 investigations, and the training and experience of other law enforcement officers with
3 whom I have had discussions, I know that there are certain characteristics common to
4 individuals involved in child pornography:

5 a. Those who receive and attempt to receive child pornography may
6 receive sexual gratification, stimulation, and satisfaction from contact with children; or
7 from fantasies they may have viewing children engaged in sexual activity or in sexually
8 suggestive poses, such as in person, in photographs, or other visual media; or from
9 literature describing such activity.

10 b. Those who receive and attempt to receive child pornography may
11 collect sexually explicit or suggestive materials in a variety of media, including
12 photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or
13 other visual media. Such individuals often times use these materials for their own sexual
14 arousal and gratification. Further, they may use these materials to lower the inhibitions
15 of children they are attempting to seduce, to arouse the selected child partner, or to
16 demonstrate the desired sexual acts. These individuals may keep records, to include
17 names, contact information, and/or dates of these interactions, of the children they have
18 attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

19 c. Those who receive and attempt to receive child pornography often
20 possess and maintain their "hard copies" of child pornographic material, that is, their
21 pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing
22 lists, books, tape recordings, etc., in the privacy and security of their home or some other
23 secure location. These individuals typically retain these "hard copies" of child
24 pornographic material for many years.

25 d. Likewise, those who receive and attempt to receive child
26 pornography often maintain their collections that are in a digital or electronic format in a
27 safe, secure and private environment, such as a computer and surrounding area. These
28 collections are often maintained for several years and are kept close by, usually at the

1 individual's residence, to enable the collector to view the collection, which is valued
2 highly.

3 e. Those who receive and attempt to receive child pornography also
4 may correspond with and/or meet others to share information and materials; rarely
5 destroy correspondence from other child pornography distributors/collectors; conceal
6 such correspondence as they do their sexually explicit material; and often maintain lists
7 of names, addresses, and telephone numbers of individuals with whom they have been in
8 contact and who share the same interests in child pornography.

9 f. Those who receive and attempt to receive child pornography prefer
10 not to be without their child pornography for any prolonged time period. This behavior
11 has been documented by law enforcement officers involved in the investigation of child
12 pornography throughout the world.

13 34. Based on my training and experience, and that of computer forensic agents
14 that I work and collaborate with on a daily basis, I know that every type and kind of
15 information, data, record, sound or image can exist and be present as electronically stored
16 information on any of a variety of computers, computer systems, digital devices, and
17 other electronic storage media. I also know that electronic evidence can be moved easily
18 from one digital device to another. As a result, I believe that electronic evidence may be
19 stored on any digital device present at the SUBJECT PREMISES and on EVINLYLE's
20 PHONES.

21 35. Based on my training and experience, and my consultation with computer
22 forensic agents who are familiar with searches of computers, I know that in some cases
23 the items set forth in Attachments B1 and B3 may take the form of files, documents, and
24 other data that is user generated and found on a digital device. In other cases, these items
25 may take the form of other types of data – including in some cases data generated
26 automatically by the devices themselves.

27 36. Based on my training and experience, and my consultation with computer
28 forensic agents who are familiar with searches of computers, I believe that if digital

1 devices are found in the SUBJECT PREMISES , there is probable cause to believe that
2 the items set forth in Attachment B1 will be stored in those digital devices, as well as
3 probable cause to believe that the items set forth in Attachment B3 will be found on
4 EVINLYLE's PHONES, for a number of reasons, including but not limited to the
5 following:

6 a. Once created, electronically stored information (ESI) can be stored
7 for years in very little space and at little or no cost. A great deal of ESI is created, and
8 stored, moreover, even without a conscious act on the part of the device operator. For
9 example, files that have been viewed via the Internet are sometimes automatically
10 downloaded into a temporary Internet directory or "cache," without the knowledge of the
11 device user. The browser often maintains a fixed amount of hard drive space devoted to
12 these files, and the files are only overwritten as they are replaced with more recently
13 viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may
14 include relevant and significant evidence regarding criminal activities, but also, and just
15 as importantly, may include evidence of the identity of the device user, and when and
16 how the device was used. Most often, some affirmative action is necessary to delete ESI.
17 And even when such action has been deliberately taken, ESI can often be recovered,
18 months or even years later, using forensic tools.

19 b. Wholly apart from data created directly (or indirectly) by user
20 generated files, digital devices – in particular, a computer's internal hard drive – contain
21 electronic evidence of how a digital device has been used, what it has been used for, and
22 who has used it. This evidence can take the form of operating system configurations,
23 artifacts from operating systems or application operations, file system data structures, and
24 virtual memory "swap" or paging files. Computer users typically do not erase or delete
25 this evidence, because special software is typically required for that task. However, it is
26 technically possible for a user to use such specialized software to delete this type of
27 information – and, the use of such special software may itself result in ESI that is relevant
28 to the criminal investigation. Secret Service agents in this case have specialized

1 knowledge and training in computers, networks, and Internet communications. In
2 particular, to properly retrieve and analyze electronically stored (computer) data, and to
3 ensure accuracy and completeness of such data and to prevent loss of the data either from
4 accidental or programmed destruction, it is necessary to conduct a forensic examination
5 of the computers. To effect such accuracy and completeness, it may also be necessary to
6 analyze not only data storage devices, but also peripheral devices which may be
7 interdependent, the software to operate them, and related instruction manuals containing
8 directions concerning operation of the computer and software.

9 **PROTOCOL FOR SORTING SEIZABLE ELECTRONICALLY STORED**
10 **INFORMATION FROM THE SUBJECT EMAIL ACCOUNT**

11 37. In order to insure that agents are limited in their search only to the contents
12 of the SUBJECT EMAIL ACCOUNT and any attachments, stored instant messages,
13 stored voice messages, documents, and photographs associated therewith; in order to
14 protect the privacy interests of other third parties who have accounts at Google; and in
15 order to minimize disruptions to normal business operations of Google; this application
16 seeks authorization to permit agents and employees of Google to assist in the execution
17 of the warrant, pursuant to 18 U.S.C. § 2703(g), as follows:

18 a. The search warrant will be presented to Google, with direction that it
19 identify and isolate the SUBJECT EMAIL ACCOUNT and associated records described
20 in Section I of Attachment B2.

21 b. Google will also be directed to create an exact duplicate in electronic
22 form of the SUBJECT EMAIL ACCOUNT and associated records specified in Section I
23 of Attachment B2, including an exact duplicate of the content of all email messages
24 stored in the SUBJECT EMAIL ACCOUNT.

25 c. Google shall then provide an exact digital copy of the contents of the
26 SUBJECT EMAIL ACCOUNT, as well as all other records associated with the account,
27 to me, or to any other Secret Service agent. Once the digital copy has been received from
28 Google, that copy will, in turn, be forensically imaged and only that image will be

1 reviewed and analyzed to identify communications and other data subject to seizure
2 pursuant to Section II of Attachment B2. The original digital copy will be sealed and
3 maintained to establish authenticity, if necessary.

4 d. I, and /or other Secret Service agents, will thereafter review the
5 forensic image, and identify from among that content those items that come within the
6 items identified in Section II to Attachment B2, for seizure. I, and/or other Secret Service
7 agents will then copy those items identified for seizure to separate media for future use in
8 investigation and prosecution. The forensic copy of the complete content of the email
9 account will also then be sealed and retained by the Secret Service, and will not be
10 unsealed absent Court authorization, except for the purpose of duplication of the entire
11 image in order to provide it, as discovery, to a charged defendant.

12 38. Analyzing the data contained in the forensic image may require special
13 technical skills, equipment, and software. It could also be very time-consuming.
14 Searching by keywords, for example, can yield thousands of "hits," each of which must
15 then be reviewed in context by the examiner to determine whether the data is within the
16 scope of the warrant. Merely finding a relevant "hit" does not end the review process.
17 Keywords used originally need to be modified continuously, based on interim results.
18 Certain file formats, moreover, do not lend themselves to keyword searches, as keywords
19 search text, and many common electronic mail, database, and spreadsheet applications
20 (which may be attached to email) do not store data as searchable text. The data is saved,
21 instead, in proprietary non-text format. And, as the volume of storage allotted by service
22 providers increases, the time it takes to properly analyze recovered data increases as well.
23 Consistent with the foregoing, searching the recovered data for the information subject to
24 seizure pursuant to this warrant may require a range of data analysis techniques and may
25 take weeks or even months.

26 39. Based upon my experience and training, and the experience and training of
27 other agents with whom I have communicated, it is necessary to seize all emails, chat
28 logs and documents, that identify any users of the subject account and any emails sent or

1 received in temporal proximity to incriminating emails that provide context to the
2 incriminating communications.

3 40. All forensic analysis of the image data will employ only those search
4 protocols and methodologies reasonably designed to identify and seize the items
5 identified in Section II of Attachment B2 to the warrant.

6 **SEARCH AND/OR SEIZURE OF DIGITAL DEVICES FROM THE SUBJECT**
7 **PREMISES AND SEARCH AND/OR SEIZURE OF EVINLYLE's PHONES**

8 41. In addition, based on my training and experience and that of computer
9 forensic agents that I work and collaborate with on a daily basis, I know that in most
10 cases it is impossible to successfully conduct a complete, accurate, and reliable search for
11 electronic evidence stored on a digital device during the physical search of a search site
12 for a number of reasons, including but not limited to the following:

13 a. Technical Requirements: Searching digital devices for criminal
14 evidence is a highly technical process requiring specific expertise and a properly
15 controlled environment. The vast array of digital hardware and software available
16 requires even digital experts to specialize in particular systems and applications, so it is
17 difficult to know before a search which expert is qualified to analyze the particular
18 system(s) and electronic evidence found at a search site. As a result, it is not always
19 possible to bring to the search site all of the necessary personnel, technical manuals, and
20 specialized equipment to conduct a thorough search of every possible digital
21 device/system present. In addition, electronic evidence search protocols are exacting
22 scientific procedures designed to protect the integrity of the evidence and to recover even
23 hidden, erased, compressed, password protected, or encrypted files. Since ESI is
24 extremely vulnerable to inadvertent or intentional modification or destruction (both from
25 external sources or from destructive code embedded in the system such as a "booby
26 trap"), a controlled environment is often essential to ensure its complete and accurate
27 analysis.
28

1 b. Volume of Evidence: The volume of data stored on many digital
2 devices is typically so large that it is impossible to search for criminal evidence in a
3 reasonable period of time during the execution of the physical search of a search site. A
4 single megabyte of storage space is the equivalent of 500 double spaced pages of text. A
5 single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double
6 spaced pages of text. Computer hard drives are now being sold for personal computers
7 capable of storing up to two terabytes (2,000 gigabytes of data.) Additionally, this data
8 may be stored in a variety of formats or may be encrypted (several new commercially
9 available operating systems provide for automatic encryption of data upon shutdown of
10 the computer).

11 c. Search Techniques: Searching the ESI for the items described in
12 Attachments B1 and B3 may require a range of data analysis techniques. In some cases,
13 it is possible for agents and analysts to conduct carefully targeted searches that can locate
14 evidence without requiring a time consuming manual search through unrelated materials
15 that may be commingled with criminal evidence. In other cases, however, such
16 techniques may not yield the evidence described in the warrant, and law enforcement
17 personnel with appropriate expertise may need to conduct more extensive searches, such
18 as scanning areas of the disk not allocated to listed files, or peruse every file briefly to
19 determine whether it falls within the scope of the warrant.

20 42. In this particular case, the government anticipates the use of a hash value
21 library to exclude normal operating system files that do not need to be searched, which
22 will facilitate the search for evidence that does come within the items described in
23 Attachments B1 and B3. Further, the government anticipates the use of hash values and
24 known file filters to assist the digital forensics examiners/agents in identifying known and
25 or suspected child pornography image files. Use of these tools will allow for the quick
26 identification of evidentiary files but also assist in the filtering of normal system files that
27 would have no bearing on the case.

1 43. In accordance with the information in this Affidavit, law enforcement
2 personnel will execute the search of digital devices seized from the SUBJECT
3 PREMISES and the search of EVINLYLE's PHONES pursuant to this warrant as
4 follows:

5 a. Upon securing the search site, the search team will conduct an initial
6 review of any digital devices/systems to determine whether the ESI contained therein can
7 be searched and/or duplicated on site in a reasonable amount of time and without
8 jeopardizing the ability to accurately preserve the data.

9 b. If, based on their training and experience, and the resources
10 available to them at the search site, the search team determines it is not practical to make
11 an onsite search, or to make an onsite copy of the ESI within a reasonable amount of time
12 and without jeopardizing the ability to accurately preserve the data, then the digital
13 devices will be seized and transported to an appropriate law enforcement laboratory for
14 review and to be forensically copied ("imaged"), as appropriate.

15 c. In order to examine the ESI in a forensically sound manner, law
16 enforcement personnel with appropriate expertise will produce a complete forensic
17 image, if possible and appropriate, of any digital device that is found to contain data or
18 items that fall within the scope of Attachments B1 and B3 of this Affidavit. In addition,
19 appropriately trained personnel may search for and attempt to recover deleted, hidden, or
20 encrypted data to determine whether the data fall within the list of items to be seized
21 pursuant to the warrant. In order to search fully for the items identified in the warrant,
22 law enforcement personnel, which may include investigative agents, may then examine
23 all of the data contained in the forensic image/s and/or on the digital devices to view their
24 precise contents and determine whether the data fall within the list of items to be seized
25 pursuant to the warrant.

26 d. The search techniques that will be used will be only those
27 methodologies, techniques and protocols as may reasonably be expected to find, identify,
28

1 segregate and/or duplicate the items authorized to be seized pursuant to Attachments B1
2 and B3 to this Affidavit.

3 e. If, after conducting its examination, law enforcement personnel
4 determine that any digital device is an instrumentality of the criminal offenses referenced
5 above, the government may retain that device during the pendency of the case as
6 necessary to, among other things, preserve the instrumentality evidence for trial, ensure
7 the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel
8 determine that a device was not an instrumentality of the criminal offenses referenced
9 above, it shall be returned to the person/entity from whom it was seized within 90 days of
10 the issuance of the warrant, unless the government seeks and obtains authorization from
11 the court for its retention.

12 44. In order to search for ESI that falls within the list of items to be seized
13 pursuant to Attachments B1 and B3 to this Affidavit, law enforcement personnel will
14 seize and search the following items (heretofore and hereinafter referred to as "digital
15 devices"), subject to the procedures set forth above:

16 a. EVINLYLE's PHONES, more fully described in Attachment A3;

17 b. Any digital device capable of being used to commit, further, or store
18 evidence of the offense(s) listed above;

19 c. Any digital device used to facilitate the transmission, creation,
20 display, encoding, or storage of data, including word processing equipment, modems,
21 docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

22 d. Any magnetic, electronic, or optical storage device capable of
23 storing data, such as disks, tapes, CD ROMs, CD Rs, CD RWs, DVDs, printer or memory
24 buffers, smart cards, PC cards, memory sticks, flashdrives, thumb drives, camera memory
25 cards, media cards, electronic notebooks, and personal digital assistants;

26 e. Any documentation, operating logs and reference manuals regarding
27 the operation of the digital device, or software;

1 f. Any applications, utility programs, compilers, interpreters, and other
2 software used to facilitate direct or indirect communication with the device hardware, or
3 ESI to be searched;

4 g. Any physical keys, encryption devices, dongles and similar physical
5 items that are necessary to gain access to the digital device, or ESI; and

6 h. Any passwords, password files, test keys, encryption codes or other
7 information necessary to access the digital device or ESI.

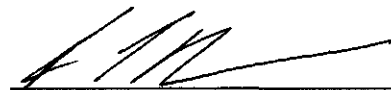
8 INSTRUMENTALITIES

9 45. Based on the information in this Affidavit, I also believe that the digital
10 device(s) at the SUBJECT PREMISES and EVINLYLE's PHONES are instrumentalities
11 of crime and constitute the means by which violations of 18 U.S.C. §§ 2251(a)
12 (Production of Child Pornography), 2252(a)(2) (Receipt and Distribution of Child
13 Pornography), and 2252(a)(4)(B) (Possession of Child Pornography) have been
14 committed. Therefore, I believe that in addition to seizing the digital devices and phones
15 to conduct a search of their contents as set forth herein, there is probable cause to seize
16 those digital devices and phones as instrumentalities of criminal activity.

17 CONCLUSION

18 46. Based on the foregoing, I believe there is probable cause that evidence,
19 fruits, and/or instrumentalities of violations of 18 U.S.C. §§ 2251(a) (Production of Child
20 Pornography), 2252(a)(2) (Receipt or Distribution of Child Pornography), and
21 2252(a)(4)(B) (Possession of Child Pornography) are (1) located at the SUBJECT
22 PREMISES, as more fully described in Attachment A1 to this Affidavit; (2) will be found
23 in the electronically stored information or communications contained and associated with
24 the SUBJECT EMAIL ACCOUNT, as more fully described in Attachment A2 to this
25 Affidavit; and (3) will be found on EVINLYLE's PHONES, as more fully described in
26 Attachment A3 to this Affidavit. I therefore request that the Court issue a warrant
27 authorizing a search of the SUBJECT PREMISES for the items more fully described in
28 Attachment B1 to this Affidavit, incorporated herein by reference, and the seizure of any

1 such items found therein. I further request that the Court issue a warrant authorizing a
2 search of the SUBJECT EMAIL ACCOUNT for the items more fully described in
3 Section I of Attachment B2 hereto, incorporated herein by reference, and the seizure of
4 the data, documents, and records identified in Section II of Attachment B2. I further
5 request that the Court issue a warrant authorizing the search of EVINLYLE's PHONES
6 for the items more fully described in Attachment B3 to this Affidavit, incorporated herein
7 by reference, and the seizure of any such items found therein.

8
9
10 

11 BRYAN MOLNAR, Affiant
12 Special Agent
13 United States Secret Service
14

15 SUBSCRIBED AND SWORN before me this 3^d day of February, 2014.
16

17 

18 KAREN L. STROMBOM
19 United States Magistrate Judge
20
21
22
23
24
25
26
27
28

ATTACHMENT A1
SUBJECT PREMISES TO BE SEARCHED

The location to be searched, 2015 68th Ave NE, Tacoma, Washington 98422 (the SUBJECT PREMISES), is more fully described as a single-family one story residence located at 2015 68th Ave NE, Tacoma, Washington 98422. The SUBJECT PREMISES is white in color with wood trim. The numbers "2015" are on the front of the residence near the front door. The SUBJECT PREMISES is located at the curve of the street where 68th Ave NE turns into 21st St NE, on the east side of the street. The garage door is red with horizontal and vertical white trim lines.

The search is to include all rooms, attics, and all other parts therein, surrounding garages or storage rooms, attached or detached, any treehouse or other similar structure, and any digital device(s) found therein.

ATTACHMENT A2
THE SUBJECT EMAIL ACCOUNT TO BE SEARCHED

The electronically stored information (and any attachments, stored messages, files, documents, and photographs associated therewith) contained in, and associated with, the Google email (gmail) account "kaiden.evinlyle@gmail.com" (hereinafter the "SUBJECT EMAIL ACCOUNT"), as well as all other user and log records associated with the SUBJECT EMAIL ACCOUNT, to include the IIS (Internet Information Services) logs associated with any linked Google Drive accounts, which are located at premises owned, maintained, controlled or operated by Google, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT A3
THINGS TO BE SEARCHED

The below-listed items were taken from KAIDEN EVINLYLE when he was booked into the Pierce County Jail on November 6, 2013. These items, collectively referred to as EVINLYLE's PHONES, are presently located at the Pierce County Jail in Tacoma, Washington:

- a. One black Samsung Galaxy Note 2 phone; and
- b. One red and white Samsung phone.

Both of EVINLYLE's PHONES bear markings on them indicating that they were purchased from T-Mobile.

**ATTACHMENT B1
SECTION 1
ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as but not limited to compact discs, CD ROMs, DVDs, smart cards, thumb drives, camera memory cards, SD cards, SIM cards, electronic notebooks, or any other storage medium) that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. §§ 2251(a) (Production of Child Pornography), 2252(a)(2) (Receipt or Distribution of Child Pornography), and 2252(a)(4)(B) (Possession of Child Pornography), which may be found at the SUBJECT PREMISES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct in any format or media, including visual depictions purchased from the website "nudistwonderland.com";

2. Evidence of the use of a PayPal account linked to the email address "kaiden.evinlyle@gmail.com," including a transaction made on July 18, 2013, in the amount of \$50.00 from the website "nudistwonderland.com";

3. Evidence of the use of the email address "kaiden.evinlyle@gmail.com";

4. Evidence of the use of the IP addresses 184.78.176.135 and 172.56.33.150;

5. Letters, email, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

6. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

7. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

1 8. Any and all address books, names, lists of names, telephone numbers, and
2 addresses of minors;

3 9. Any and all diaries, notebooks, notes, non-pornographic pictures of
4 children, and any other records reflecting personal contact or other activities with minors;

5 10. Digital devices and/or their components, which include, but are not limited
6 to:

7 a. Any digital devices and storage device capable of being used to
8 commit, further, or store evidence of the offense listed above;

9 b. Any digital devices used to facilitate the transmission, creation,
10 display, encoding or storage of data, including word processing equipment, modems,
11 docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

12 c. Any magnetic, electronic, or optical storage device capable of
13 storing data, such as disks, tapes, CD ROMs, CD Rs, CD RWs, DVDs, printer or memory
14 buffers, smart cards, PC cards, memory sticks, flashdrives, thumb drives, camera memory
15 cards, media cards, SD cards, SIM cards, electronic notebooks, and personal digital
16 assistants;

17 d. Any documentation, operating logs and reference manuals regarding
18 the operation of the digital device or software;

19 e. Any applications, utility programs, compilers, interpreters, and other
20 software used to facilitate direct or indirect communication with the computer hardware,
21 storage devices, or data to be searched;

22 f. Any physical keys, encryption devices, dongles and similar physical
23 items that are necessary to gain access to the computer equipment, storage devices or
24 data; and

25 g. Any passwords, password files, test keys, encryption codes or other
26 information necessary to access the computer equipment, storage devices or data;

1 11. Evidence of who used, owned or controlled any seized digital device(s) at
2 the time the things described in this warrant were created, edited, or deleted, such as logs,
3 registry entries, saved user names and passwords, documents, and browsing history;

4 12. Evidence of malware that would allow others to control any seized digital
5 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
6 as evidence of the presence or absence of security software designed to detect malware;
7 as well as evidence of the lack of such malware;

8 13. Evidence of the attachment to the digital device(s) of other storage devices
9 or similar containers for electronic evidence;

10 14. Evidence of counter forensic programs (and associated data) that are
11 designed to eliminate data from a digital device;

12 15. Evidence of times the digital device(s) was used;

13 16. Any other ESI from the digital device(s) necessary to understand how the
14 digital device was used, the purpose of its use, who used it, and when.

15 **SECTION 2**
16 **SEARCH TECHNIQUES**

17 Searching the electronically stored information (ESI) for the items described in
18 Section 1, paragraphs 1-9 and 11-16, of this Attachment B may require a range of data
19 analysis techniques. In some cases, it is possible for agents and analysts to conduct
20 carefully targeted searches that can locate evidence without requiring a time consuming
21 manual search through unrelated materials that may be commingled with criminal
22 evidence. In other cases, however, such techniques may not yield the evidence described
23 in the warrant, and law enforcement personnel with appropriate expertise may need to
24 conduct more extensive searches, such as scanning areas of the disk not allocated to listed
25 files, or peruse every file briefly to determine whether it falls within the scope of the
26 warrant.

27 In this particular case, the government anticipates the use of a hash value library to
28 exclude normal operating system files that do not need to be searched, which will

1 facilitate the search for evidence that does come within the items described in Section 1,
2 paragraphs 1-9 and 11-16, of this Attachment B. Further, the government anticipates the
3 use of hash values and known file filters to assist the digital forensics examiners/agents in
4 identifying known and or suspected child pornography image files. Use of these tools
5 will allow for the quick identification of evidentiary files but also assist in the filtering of
6 normal system files that would have no bearing on the case.

7 Thus, law enforcement personnel are authorized to execute the search of digital
8 devices seized pursuant to this warrant as follows:

9 a. Upon securing the search site, the search team will conduct an initial
10 review of any digital devices/systems to determine whether the ESI contained therein can
11 be searched and/or duplicated on site in a reasonable amount of time and without
12 jeopardizing the ability to accurately preserve the data.

13 b. If, based on their training and experience, and the resources
14 available to them at the search site, the search team determines it is not practical to make
15 an onsite search, or to make an onsite copy of the ESI within a reasonable amount of time
16 and without jeopardizing the ability to accurately preserve the data, then the digital
17 devices will be seized and transported to an appropriate law enforcement laboratory for
18 review and to be forensically copied ("imaged"), as appropriate.

19 c. In order to examine the ESI in a forensically sound manner, law
20 enforcement personnel with appropriate expertise will produce a complete forensic
21 image, if possible and appropriate, of any digital device that is found to contain data or
22 items that fall within the scope of Section 1, paragraphs 1-9 and 11-16, of this
23 Attachment B. In addition, appropriately trained personnel may search for and attempt to
24 recover deleted, hidden, or encrypted data to determine whether the data fall within the
25 list of items to be seized pursuant to the warrant. In order to search fully for the items
26 identified in the warrant, law enforcement personnel may then examine all of the data
27 contained in the forensic image/s and/or on the digital devices to view their precise
28

1 contents and determine whether the data fall within the list of items to be seized pursuant
2 to the warrant.

3 d. The search techniques that will be used will be only those
4 methodologies, techniques and protocols as may reasonably be expected to find, identify,
5 segregate and/or duplicate the items authorized to be seized pursuant to Section 1,
6 paragraphs 1-9 and 11-16, of this Attachment B.

7 e. If, after conducting its examination, law enforcement personnel
8 determine that any digital device is an instrumentality of the criminal offenses referenced
9 above, the government may retain that device during the pendency of the case as
10 necessary to, among other things, preserve the instrumentality evidence for trial, ensure
11 the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel
12 determine that a device was not an instrumentality of the criminal offenses referenced
13 above, it shall be returned to the person/entity from whom it was seized within 90 days of
14 the issuance of the warrant, unless the government seeks and obtains authorization from
15 the court for its retention.

16
17 **THE SEIZURE OF DIGITAL DEVICES AND/OR THEIR COMPONENTS AS**
18 **SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH**
19 **WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES**
20 **CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY**
21 **DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF CONDUCTING OFF**
22 **SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE,**
23 **INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.**
24
25
26
27
28

**ATTACHMENT B2
ITEMS TO BE SEIZED**

Section I - Items to be to be Provided by Google for Search

1. All electronically stored information and communications contained in and associated with the Google email (gmail) account "kaiden.evinlyle@gmail.com" (hereinafter the "SUBJECT EMAIL ACCOUNT"), including any attachments, stored messages, files, documents, and photographs, account registration information, user contact information, linked web addresses, and logs, from February 28, 2007, to present;

All electronically stored information and communications contained in the SUBJECT EMAIL ACCOUNT, including any Picasa Web Albums account(s) linked to the SUBJECT EMAIL ACCOUNT and any Google Drive cloud storage account(s) linked to the SUBJECT EMAIL ACCOUNT, and all account registration information, user contact information, linked web addresses and posted images, content and logs, to include the IIS (Internet Information Services) logs associated with the Google Drive accounts;

2. All subscriber records associated with the SUBJECT EMAIL ACCOUNT, including name, address, records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, (including any temporarily assigned network address), and means and source of payment for such service, including any credit card or bank account number;

3. Any and all other log records, including IP address captures, associated with the SUBJECT EMAIL ACCOUNT;

4. Any address lists or buddy/contact lists associated with the SUBJECT EMAIL ACCOUNT; and

5. Any records of communications between Google, and any other person about issues relating to the SUBJECT EMAIL ACCOUNT, such as technical problems, billing inquiries, or complaints from other users about the SUBJECT EMAIL

1 ACCOUNT. This is to include records of contacts between the subscriber and the
2 provider's support services, as well as records of any actions taken by the provider or
3 subscriber as a result of the communications.

4 **Section II - Items to be Seized**

5 From all electronically stored information and communications contained in the
6 SUBJECT EMAIL ACCOUNT, including any Picasa Web Album account(s) and Google
7 Drive cloud storage account(s) linked to the SUBJECT EMAIL ACCOUNT:

8 a. All messages, documents, and profile information, attachments, or
9 other data that serves to identify any persons who use or access the SUBJECT EMAIL
10 ACCOUNT, or who exercise in any way any dominion or control over the SUBJECT
11 EMAIL ACCOUNT;

12 b. Any address lists or buddy/contact lists associated with the
13 SUBJECT EMAIL ACCOUNT;

14 c. All images of child pornography and any messages, documents and
15 profile information, attachments, or other data that refer to child pornography or the
16 possession, receipt, distribution, or production of child pornography;

17 d. All subscriber records associated with the SUBJECT EMAIL
18 ACCOUNT, including name, address, records of session times and durations, length of
19 service (including start date) and types of service utilized, telephone or instrument
20 number or other subscriber number or identity, (including any temporarily assigned
21 network address), and means and source of payment for such service, including any
22 credit card or bank account number;

23 e. Any and all other log records, including IP address captures,
24 associated with the SUBJECT EMAIL ACCOUNT; and

25 f. Any records of communications between Google and any person
26 about issues relating to the SUBJECT EMAIL ACCOUNT, such as technical problems,
27 billing inquiries, or complaints from other users. This is to include records of contacts
28

1 between the subscriber and the provider's support services, as well as records of any
2 actions taken by the provider or subscriber as a result of the communications.

**ATTACHMENT B3
SECTION 1
ITEMS TO BE SEIZED**

The following records, documents, files, or materials that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. §§ 2251(a) (Production of Child Pornography), 2252(a)(2) (Receipt or Distribution of Child Pornography), and 2252(a)(4)(B) (Possession of Child Pornography) which may be found on EVINLYLE's PHONES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct in any format or media, including visual depictions purchased from the website "nudistwonderland.com";

2. Evidence of the use of a PayPal account linked to the email address "kaiden.evinlyle@gmail.com," including a transaction made on July 18, 2013, in the amount of \$50.00 from the website "nudistwonderland.com";

3. Evidence of the use of the email address "kaiden.evinlyle@gmail.com";

4. Evidence of the use of the IP addresses 184.78.176.135 and 172.56.33.150;

5. Email, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

6. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

7. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

8. Any and all address books, names, lists of names, telephone numbers, and addresses of minors;

9. Any and all diaries, notebooks, notes, non-pornographic pictures of children, and any other records reflecting personal contact or other activities with minors;

10. Evidence of who used, owned or controlled EVINLYLE's PHONES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

11. Evidence of malware that would allow others to control EVINLYLE's PHONES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

12. Evidence of counter forensic programs (and associated data) that are designed to eliminate data from a digital device;

13. Evidence of times and dates EVINLYLE's PHONES were used;

14. Any other electronically stored information (ESI) from EVINLYLE's PHONES necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

SECTION 2 SEARCH TECHNIQUES

Searching the ESI for the items described in Section 1 of this Attachment B3 may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement personnel with appropriate expertise may need to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant.

In this particular case, the government anticipates the use of a hash value library to exclude normal operating system files that do not need to be searched, which will facilitate the search for evidence that does come within the items described in Section 1 of this Attachment B3. Further, the government anticipates the use of hash values and

1 known file filters to assist the digital forensics examiners/agents in identifying known and
2 or suspected child pornography image files. Use of these tools will allow for the quick
3 identification of evidentiary files but also assist in the filtering of normal system files that
4 would have no bearing on the case.

5 Law enforcement personnel are authorized to execute the search of EVINLYLE's
6 PHONES, pursuant to this warrant, as follows:

7 a. In order to examine the ESI in a forensically sound manner, law
8 enforcement personnel with appropriate expertise will produce a complete forensic
9 image, if possible, of EVINLYLE's PHONES. In addition, appropriately trained
10 personnel may search for and attempt to recover deleted, hidden, or encrypted data to
11 determine whether the data fall within the list of items to be seized pursuant to the
12 warrant. In order to search fully for the items identified in the warrant, law enforcement
13 personnel, which may include the investigative agents, may then examine all of the data
14 contained in the forensic image/s and/or on the digital devices to view their precise
15 contents and determine whether the data fall within the list of items to be seized pursuant
16 to the warrant.

17 b. The search techniques that will be used will be only those
18 methodologies, techniques and protocols as may reasonably be expected to find, identify,
19 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B3 to
20 this Affidavit.

21 c. If, after conducting its examination, law enforcement personnel
22 determine that either of EVINLYLE's PHONES is an instrumentality of the criminal
23 offenses referenced above, the government may retain that device during the pendency of
24 the case as necessary to, among other things, preserve the instrumentality evidence for
25 trial, ensure the chain of custody, and litigate the issue of forfeiture. If law enforcement
26 personnel determine that a device was not an instrumentality of the criminal offenses
27 referenced above, it shall be returned to the person/entity from whom it was seized within
28

1 90 days of the issuance of the warrant, unless the government seeks and obtains
2 authorization from the court for its retention.